Order Code RL32594

Public Safety Communications: Policy, Proposals, Legislation and Progress

Updated June 8, 2005

Linda K. Moore
Analyst in Telecommunications Policy
Resources, Science, and Industry Division

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
08 JUN 2005	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Public Safety Communications: Policy, Proposals, Legislation and Progress	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **David D. Acker Library and Knowledge Repository Defense Acquisition University Fort Belvoir, VA**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**32**	

Public Safety Communications: Policy, Proposals, Legislation and Progress

Summary

Since September 11, 2001, the effectiveness of America's communications capabilities in support of the information needs of first responders and other public safety workers has been a matter of concern to Congress. The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) included sections that responded to recommendations made by the 9/ll Commission, in its report of July 2004, and by others in recent years, regarding public safety communications. Nonetheless, there is much still to be done to bring the United States to the threshold of adequate communications capabilities in emergencies. Congress can expect that the many advocates for public safety, in all its forms, will continue to push for improvements in public safety communications and interoperability.

This report provides an analysis of major policy questions regarding public safety communications. The 9/11 Commission recommendations for action to improve communications and the testimony and comments of experts provide a framework to review what has been accomplished since September 11, what legislative initiatives could be considered by the 109th Congress, and longer term goals and concerns. Major issues include (1) unifying spectrum policy and communications policy at every level; (2) using signal corps type skills and technology, as suggested by the 9/11 Commission, to achieve interoperability; and (3) evaluating the pace and effectiveness of federal actions taken to-date.

Congress has responded by requiring a number of studies and pilots, the results of which could shape policy decisions in the future. In particular, both Congress and the Administration have set requirements for the Department of Homeland Security that include developing a strategy for spectrum use and evaluating its role in public safety communications.

A bill (H.R. 1646) to make spectrum available for public safety has been reintroduced by Representative Jane Harman. The bill, the Homeland Emergency Response Operations Act, or HERO Act, previously introduced in the 107th and 108th Congresses, was cited by the 9/11 Commission, which recommended its passage. Many policy discussions regarding federal funding for public safety communications revolve around identifying risk-based formulas to distribute grants among states. Examples of legislation introduced to modify the way funds are distributed are S. 21 (Senator Collins) and H.R. 1544 (Representative Shays). Citing the continued lack of communications capabilities within the New York City Fire Department, H.R. 1795 (Representative Maloney) would fund a new system for the city's firefighters that would provide a network and radios incorporating many leading edge technologies and networking concepts. Taking a different approach, the Public Safety Interoperability Implementation Act (H.R. 1323, Representative Stupak) would place some spectrum auction proceeds in a trust fund to provide grants to improve public safety communications.

This report will be updated.

Contents

Public Safety Communications: Policy, Proposals, Legislation and Progress

Public safety agencies include the nation's first responders (such as firefighters, police officers, and ambulance services) and a number of local, state, federal — and sometimes regional — authorities. Communications, often wireless radios, are vital to these agencies' effectiveness and to the safety of their members and the public. Wireless technology requires radio frequency capacity in order to function, and existing wireless technology is designed to work within specified frequency ranges.

Different operations, different applications, different rules and standards, and different radio frequencies are among the problems first responders face in trying to communicate with each other. Interoperability, also referred to as compatibility or connectivity, refers to the capability for these different systems to readily contact each other. Facilitating interoperability has been a policy concern of public safety officials for a number of years.[1] Since September 11, 2001 — when communications failures added to the horror of the day — achieving interoperability for public safety communications has become an important policy concern for Congress.

I. PROGRESS AND GOALS

Intelligence Reform and Terrorism Prevention Act

The National Commission on Terrorist Attacks Upon the United States (9/11 Commission) analysis of communications difficulties on September 11, 2001 was summarized in the following recommendation.

> Congress should support pending legislation which provides for the expedited and increased assignment of radio spectrum for public safety purposes. Furthermore, high-risk urban areas such as New York City and Washington, D.C., should establish signal corps units to ensure communications connectivity between and among civilian authorities, local first responders, and the National Guard. Federal funding of such units should be given high priority by Congress.[2]

The Commission, in this paragraph, recognized the important link between access to spectrum and the effectiveness of communications technology. Briefly, the recommendation says:

---

[1] Difficulties in communications after a major plane crash in the Potomac River in January 1982 is often cited as the impetus for expanding interoperability in the Capital Area.

[2] The National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, Official Government Edition, Washington, D.C. 2004, p. 397.

- free up and assign more **spectrum** for public safety use;
- establish **communications support** (the role of a signal corps typically is to provide information systems and networks for real-time command and control);
- with **interoperable communications** (connectivity); and
- fund these communications operations for **high-risk urban areas**.

The 9/11 Commission recommendations for public safety are a pithy summation of issues raised in the last decade or so. Provisions in the act that respond to the recommendations of the Commission and of the public safety community, among others, are discussed below.

Spectrum Allocation

The Balanced Budget Act of 1997 requires the Federal Communications Commission (FCC) to allocate 24 MHz of spectrum at 700 MHz[3] to public safety, without providing a hard deadline for the transfer.[4] The channels designated for public safety are among those currently held by TV broadcasters; they are to be cleared as part of the move from analog to digital television (DTV). The 9/11 Commission report regarding spectrum availability speaks directly to the issue of the 700 MHz spectrum that has been assigned to public safety but is not yet available. It recommended that Congress pass proposed legislation (the HERO Act, see below) that would free those channels. Although the task of freeing spectrum for public safety could be addressed as a separate issue, many recent actions have focused on the steps to be taken for releasing all the encumbered spectrum while assuring access to broadcast television programs.[5]

Beginning with the 107th Congress, Representative Jane Harman has introduced in each Congress legislation that would assure the timely release of radio channels at 700 MHZ for public safety use. The Homeland Emergency Response Operations Act, or HERO Act (H.R. 1646), reintroduced in April 2005, requires the FCC to "take all actions necessary to complete assignments" for these channels so that operations could begin no later than January 1, 2007, adhering to the deadline originally envisioned for the completion of the transition to DTV for all affected channels.

---

[3] Radio frequency spectrum is measured in hertz. Radio frequency is the portion of electromagnetic spectrum that carries radio waves. The distance an energy wave takes to complete one cycle is its wavelength. Frequency is the number of wavelengths measured at a given point per unit of time, in cycles per second, or hertz (Hz). Typical designations are: kHz — kilohertz or thousands of hertz; MHz — megahertz, or millions of hertz; and GHz — gigahertz, or billions of hertz. Bandwidth refers generally to the capacity of channels to carry voice and data, a function of technology and the amount of spectrum assigned. Most frequency assignments for first responders are narrowband and most channels currently in use are located below 512 MHz.

[4] 47 U.S.C. § 309 (j) (14).

[5] For example Hearing of the House of Representatives, Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet, "The Role of Technology in Achieving a Hard Deadline for the DTV Transition," February 17, 2005.

Sense of Congress. The Intelligence Reform and Terrorism Prevention Act (P.L. 108-458) provides the sense of Congress that it "must act to pass legislation in the first session of the 109th Congress that establishes a comprehensive approach to the timely return of analog broadcast spectrum as early as December 31, 2006,"[6] and that any delay "will delay the ability of public safety entities to begin planning to use this needed spectrum."[7] Although the Senate version of the intelligence bill (S. 2845, 108th) included a provision that would have released in a timely manner those channels needed for public safety communications, the House of Representative's preference to address the issue in its entirety prevailed. Some of the possible actions that Congress may decide to take could include using spectrum auction proceeds to subsidize the purchase of set-top signal converter boxes, thereby allowing analog broadcasts to continue indefinitely without cutting viewer access;[8] endorsing plans by the FCC to change the criteria for freeing 700 MHz channels; or a rewriting of the provisions of the Balanced Budget Act that govern transition plans.[9]

Improving Spectrum Capacity for Public Safety. The act requires the FCC, in consultation with the Secretary of Homeland Security and the National Telecommunications and Information Administration (NTIA),[10] to conduct a study on the spectrum needs for public safety, including the possibility of increasing the amount of spectrum at 700 MHz.[11] This provision is responsive to the many public safety officials who believe that additional spectrum should be assigned for public safety use — and not exclusively for first responders.[12] In addition to providing spectrum for other types of users, the spectrum available for public safety should be able to support high-speed transmissions capable of quickly sending data (such as photographs, floor plans and live video). This requires providing frequencies with greater bandwidth to enable wireless broadband and new-generation technologies. Although radio frequencies have been designated for state and local public safety use in the 700 MHz range, there are no allocations specifically for federal use at 700 MHz and the bandwidth assignments are judged by most experts to be too narrow for full broadband. Many have advocated that additional spectrum be allocated at 700

---

[6] P.L. 108-458,Title VII, Subtitle E, Sec. 7501 (b) (1).

[7] P.L. 108-458,Title VII, Subtitle E, Sec. 7501 (b) (2).

[8] The Administration reportedly has opposed this approach, see, for example, "White House Opposes DTV Subsidy Proposal," by Donny Jackson, TelephonyOnline.com, October 22, 2004.

[9] Details are provided in CRS Report RL32622, *Public Safety, Interoperability and the Transition to Digital Television*.

[10] The NTIA, Department of Commerce, administers federal use of spectrum.

[11] P.L. 108-458, Title VII, Subtitle E, Sec. 7502 (a).

[12] In 1997 amendments to the Communications Act of 1934 , Congress defined public safety services as "services — (A) the sole or principal purpose of which is to protect the safety of life, health or property; (B) that are provided (i) by State or local government entities; or (ii) by nongovernmental organizations that are authorized by a governmental entity whose primary mission is the provision of such services ; and (C) that are not made commercially available to the public by the provider." [47 U.S.C. § 337 (f)(1)]. The Intelligence Reform and Terrorism Prevention Act uses the more restrictive definition of first responders as provided in the Homeland Security Act of 2002 (6 U.S.C. § 101).

MHz to accommodate federal users and to support newer, broadband wireless technologies as part of a nationwide network for public safety communications. The Spectrum Coalition for Public Safety has circulated proposed legislation that would allocate additional spectrum at 700 MHz for use by state and local first responders, critical infrastructure industries, and federal public safety agencies.[13]

Although, cumulatively, radio frequencies designated for non-federal public safety total over 90 MHz,[14] the characteristics of these frequencies are dis-similar, requiring different technological solutions. The fragmentation of spectrum assignments for public safety is a significant barrier to achieving interoperability in the future, and is presently among the technical problems that plague public safety communications, such as out-of-date equipment, proprietary solutions, congestion, and interference. The immediate barrier to achieving radio communications interoperability is — simply put — that UHF and VHF frequencies[15] cannot connect directly with each other, and that older, analog equipment widely used below 512 MHz cannot connect with newer digital equipment at 800 MHz. Technology for new frequencies at 4.9 GHz is still in the early stage of development but these frequencies appear suitable primarily for local-area (short-range) transmission. None of the above frequency assignments can, using current technology, support wide-area communications relying on high-speed, data-rich transmissions. Placing key communications capabilities, including interoperable connections, is viewed by many as the optimal solution for overcoming problems caused by incompatible radio frequencies and technologies.

Responding to Congress's requirement for a study, the FCC has begun the process with a request for comment on the future spectrum needs of emergency response providers.[16] A statement, by Commissioner Michael J. Copps, accompanying the request for comment sums up the sentiments of many of those involved in public safety.

> A useful report to Congress will: (1) include a survey of what spectrum is currently being used by which entities across the country; (2) understand that not all frequencies are the same and therefore assess whether we are matching spectrum with appropriate physical characteristics to current and future public safety needs; (3) indicate whether some bands are being underutilized because public safety needs have changed since initial allocation; (4) assess the current interference situation in public safety bands; (5) identify various approaches to

---

[13] Spectrum Coalition for Public Safety at [http://www.spectrumcoalition.org].

[14] Estimated at approximately 97 MHz in Testimony of Michael K. Powell, Chairman, Federal Communications Commission, at Hearing of Senate Committee on Commerce, Science and Transportation, "Spectrum for Public Safety Users," September 8, 2004. The NTIA has apparently not supplied a similar estimate of frequencies assigned to federal agencies that are or can be accessed for public safety purposes.

[15] Very High Frequency (VHF) and Ultra High Frequency (UHF) are transmitted in three bands in the United States — low VHF, high VHF and UHF.

[16] "Federal Communications Commission Requests Comments on Spectrum Needs of Emergency Response Providers," FCC News, March 29, 2005, WT Docket No. 05-157 at [http://www.fcc.gov].

> interoperability and their success or failure; (6) identify the current availability of interoperable channels and whether or not they are widely used and why; and (7) determine how a nationwide interoperable network can connect not only local police and fire entities, but also the FBI, DHS, FEMA, and other critical Federal agencies. I also believe that we must begin to understand that emergency rooms and the medical community are integral parts of emergency response and homeland security. If we build a system that excludes the medical community it will be dangerously incomplete.

The need for greater spectral capacity will grow with the number of participants in interoperable systems and the amounts of information being shared on these systems. Bottlenecks in communications are a problem that is already manifest among federal computer networks and landline transmissions, and many believe it will worsen as more information is pushed through. As emergency response units become more mobile, demand for time-critical, wireless communications capacity will also increase. New technologies that improve communications capacity are being introduced almost continuously, but the need to provide suitable spectrum for a full range of voice and data communications will persist.

The Cost of Fragmentation. The number of radio frequencies available for interoperable communications capability can significantly impact first responder communications, and the range of these frequencies can significantly impact the cost of equipment. Manufacturers cite short production runs for wireless handsets as one of the causes for higher costs associated with public safety communications equipment. An analog walkie-talkie might cost $300, a recent "typical" price. A radio with limited interoperability that meets Project 25 standards[17] might cost as much as $3,000 in a limited production run. The greater the number of communications devices using compatible frequencies, the greater are the opportunities for economies of scale in production, which in turn typically lowers the cost and final price on equipment. Purchasing "cross-talk" equipment — to provide interoperability by linking radio frequencies through a black box — can run into the millions of dollars. Beyond issues such as risk-assessment, prioritizing, and equity in funding programs, many within Congress and without are concerned about the long-term implications of funding short-term communications solutions, such as cross-talk equipment.[18] Many believe that the unavailability of spectrum at 700 MHz is stalling advances in technology and planning for new networks, thus adding to the short-term costs of maintaining public safety communications. Therefore, many argue that creating common, interoperable channels at 700 MHz is cost-effective as well as organizationally and technologically desirable.[19]

---

[17] Project 25 refers to the suite of standards for public safety communications under development by the Telecommunications Industry Association, a standards-setting body authorized for this program. [http://www.tiaonline.org/standards/project_25/]. Viewed April 26, 2005.

[18] For example, statements at Hearing of the House of Representatives, Committee on Homeland Security, Subcommittee on Emergency Preparedness, Science and Technology, "The Need for Grant Reform and The Faster and Smarter Funding for First Responders Act of 2005," April 13, 2005.

[19] Speakers at a CRS-sponsored seminar provided equipment cost estimates and were among (continued...)

Communications Support and Interoperability

The 9/11 Commission recommendation to use signal corps to assure connectivity in high-risk areas is apparently a reference to the Army Signal Corps. In testimony before Congress, Commissioner John F. Lehman commented on the lack of connectivity for first responders and referred to the "tremendous expertise" of the Department of Defense (DOD) and its capabilities in procurement, technology, and research and development. Referring specifically to the Army Signal Corps, Mr. Lehman suggested that the DOD should have responsibility to provide "that kind of support to the first responders in the high-target, high risk cities like New York."[20]

The role of a signal corps typically is to provide information systems and networks for real-time command and control. The Army maintains mobile units to provide capacity and specialized support to military operations, worldwide. According to the U.S. Army Info Site on the Internet

> The mission of the Signal Corps is to provide and manage communications and information systems support for the command and control of combined arms forces. Signal support includes Network Operations (information assurance, information dissemination management, and network management) and management of the electromagnetic spectrum. Signal support encompasses all aspects of designing, installing, maintaining, and managing information networks to include communications links, computers, and other components of local and wide area networks. Signal forces plan, install, operate, and maintain voice and data communications networks that employ single and multi-channel satellite, tropospheric scatter, terrestrial microwave, switching, messaging, video-teleconferencing, visual information, and other related systems. They integrate tactical, strategic and sustaining base communications, information processing and management systems into a seamless global information network that supports knowledge dominance for Army, joint and coalition operations.[21]

The Army Signal Corps is intended to provide a communications backbone, a core network, with important elements such as spectrum management, the operation of communications centers, and support of communications networks that include both large area regional communications and radio coverage for local wireless interoperability. The Corps' communication backbone delivers connectivity on site among combined forces and connectivity to command centers. These operations are scalable and can be deployed when and where needed.

---

[19] (...continued)
those who have confirmed the need for access to spectrum at 700 MHz as part of the solution for achieving interoperability. *Public Safety Communications: Interoperability Technology Workshop*, November 17, 2003.

[20] Testimony of Commissioner John F. Lehman, National Commission on Terrorist Attacks Upon the United States, Hearing, House of Representatives, Committee on Government Reform, "Moving from 'Need to Know' to 'Need to Share'," August 3, 2004.

[21] From [http://www.us-army-info.com/pages/mos/signal/signal.html]. Viewed April 13, 2005.

A discussion of key federal programs to support communications and foster interoperability is included in the Appendix of this report. At the end of the 108th Congress, the goals and accomplishments of these programs could be viewed by many as less ambitious than the signal corps template provided by the 9/11 Commission. Congress responded to recommendations for improvements with language in the Intelligence Reform and Terrorism Prevention Act that raises the bar for performance and accountability, as well as easing some of the obstacles to performance. Among the program goals the act sets for the Department of Homeland Security and the Federal Communications Commission are the following.

- Develop a comprehensive, national approach for achieving interoperability.
- Coordinate with other federal agencies.
- Establish appropriate minimum capabilities for interoperability.
- Accelerate development of voluntary standards.
- Encourage open architecture and commercial products.
- Assist other agencies with research and development.
- Prioritize within DHS for research, development, testing and related programs.
- Establish coordinated guidance for federal grant programs.
- Provide technical assistance.
- Develop and disseminate best practices.
- Establish performance measurements and milestones for systematic measurement of progress.[22]

The act also instructs the Secretary of Homeland Security to lead a study to "assess strategies that may be used to meet public safety telecommunications needs."[23] The strategies study is to address the need for nationwide interoperable communications networks, the capacity of public safety to use wireless broadband applications, and the communications capabilities of "all emergency response providers. . . ." The use of "commercial wireless technologies to the greatest extent possible" is to be considered.

Interoperability: SAFECOM. Responsibility to coordinate and rationalize federal networks, and to support interoperability, has been assigned to SAFECOM by the Office of Management and Budget (OMB) as an e-government initiative. This

---

[22] P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (a) (1).

[23] P.L. 108-458, Title VII, Subtitle E, Sec. 7502 (b).

role has been supported by the Administration[24] and confirmed by Congress with language in the National Intelligence and Terrorism Prevention Act.[25] Programs at SAFECOM, now placed within the DHS Office for Interoperability and Compatability, are primarily consultative in nature and focused on administrative issues. While it makes important contributions to testing equipment and working on technical and operational standards for interoperable equipment, SAFECOM does not appear to be planning for a standardized network overlay that can encompass the many useful, but mostly not connected, networks that already play vital roles in public safety communications.

Interoperability: Integrated Wireless Network. Separately, an Integrated Wireless Network (IWN) for law enforcement is being planned as a joint program by the Departments of Justice, the Treasury, and Homeland Security. DHS is represented in the IWN Joint Program Office through the Wireless Management Office of the Chief Information Officer.[26] IWN, from its description, will have limited interoperability at the state and local level. The described objective of IWN is network integration for "the nation's law enforcement wireless communication, and data exchange capability through the use of a secure integrated wireless network."[27] Most of the parameters of the IWN program — equipment, technologies, standards, use of spectrum, etc. — will be established through the final choice of vendor or vendors and the network solutions proposed. There are some specific requirements, such as for open standards or standards that are readily available to all — such as Project 25 — [28] and use of VHF frequencies already assigned to federal users.[29] Currently, the program has selected five companies as semi-finalists.[30] These companies have been asked to submit a detailed system

---

[24] Testimony of Karen S. Evans, E-Gov/IT Director, Office of Management and Budget, Hearing of the House of Representatives, Committee on Government Reform, Joint Hearing, Subcommittee on National Security, Emerging Threats and International Relations and Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, "Public Safety Interoperability: Can You Hear Me Now?," November 6, 2003.

[25] P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (a) (2).

[26] Memorandum of Understanding Between the Department of Homeland Security, the Department of Justice, and the Department of the Treasury Regarding a Joint Tactical Wireless Communications System, at [http://www.usdoj.gov/jmd/iwn/schedule.html]. Viewed April 14, 2005.

[27] Request for Comment, Draft Phase 2 Request for Proposals, October 13, 2004, C.2.3 (a), page 8 at [http://www.usdoj.gov/jmd/iwn/schedule.html]. Viewed April 14, 2005.

[28] Request for Comment, Draft Phase 2 Request for Proposals, October 13, 2004, C.2.1 (d), page 8 at [http://www.usdoj.gov/jmd/iwn/schedule.html]. Viewed April 14, 2005.

[29] Presentation by Michael Duffy, Deputy Chief Information Officer, E-Gov, Department of Justice, at Integrated Wireless Network (IWN) Industry Day, April 27, 2004.

[30] They are: AT&T, Boeing, General Dynamics, Lockheed Martin and Motorola. From Results of the IWN Phase I Downselect at [http://www.usdoj.gov/jmd/iwn/schedule.html]. Viewed April 14, 2005.

design and an implementation plan[31] and are encouraged to provide "innovative, big-picture, solution sets."[32] The departmental objectives for coverage are: major metropolitan areas; major highways; U.S. land and sea border areas; and ports of entry.[33] The reported estimated cost for IWN is $10 billion.[34] Funding is provided jointly from budgeted sums designated for the upgrading of communications equipment to meet NTIA requirements for narrowbanding and interoperability.[35] Although the network being sought is intended to serve law enforcement users within the three sponsoring departments, descriptions of the program invoke the possibility that IWN will provide the template for national interoperability.[36]

Interoperability: First Responders. In terms of achieving interoperability for the nation's first responders, the deployment of IWN could be viewed by some as a glass that is either half empty or half full. Among the positive contributions that IWN will provide to public safety communications are: the eventual adoption, on a massive scale, of a network architecture that can be emulated by all — presumedly with standardized interfaces; coordination of communications and interoperability among important components of homeland security; and significant improvements in communications technology and the efficient use of spectrum.

There could be questions as to how this project, running parallel with plans from the Office of Interoperability and Compatibility, will impact the goal that Congress has set for nationwide interoperability. Will it, for example, delay work on standards development until the process of vendor selection is complete and the standards for IWN have been fully established? Will the proposed interface between federal law enforcement personnel and selected state and local officials be extendable to, say, interoperability between those officials and local firefighters or EMS personnel? Should other federal networks be built along functional lines and then linked with IWN, possibly providing the connectivity needed at the state and local level among different types of responders? Will there be a link to emergency alert and warning systems? The specification to use federal frequencies apparently solves the problem

---

[31] Request for Comment, Draft Phase 2 Request for Proposals, October 13, 2004, A.4 (a), page 3 at [http://www.usdoj.gov/jmd/iwn/schedule.html]. Viewed April 14, 2005.

[32] Request for Comment, Draft Phase 2 Request for Proposals, October 13, 2004, C.2.1(c), page 7 at [http://www.usdoj.gov/jmd/iwn/schedule.html]. Viewed April 14, 2005.

[33] Request for Comment, Draft Phase 2 Request for Proposals, October 13, 2004, C.2.1. (c), page 7 at [http://www.usdoj.gov/jmd/iwn/schedule.html]. Viewed April 14, 2005.

[34] "Massive Federal Wireless Project Delayed," by Wilson P. Dizard III, GCN, March 30, 2005.

[35] Memorandum of Understanding Between the Department of Homeland Security, the Department of Justice, and the Department of the Treasury Regarding a Joint Tactical Wireless Communications System, and Presentation by Michael Duffy, Deputy Chief Information Officer, E-Gov, Department of Justice, at Integrated Wireless Network (IWN) Industry Day, April 27, 2004.

[36] "The successful deployment and operation of IWN will be a key enabler for national coordination capability," in Request for Comment, Draft Phase 2 Request for Proposals, October 13, 2004, C.2.5 (b) (1) (F), page 10 at [http://www.usdoj.gov/jmd/iwn/schedule.html]. Viewed April 14, 2005.

of spectrum access for IWN but does not appear to move toward the solution to the vexing problem of providing suitable radio frequencies for interoperability for first responders. The frequencies that IWN is to use are the same frequencies that were generally not available to those responding to terrorist attacks on September 11, 2001.

Funding

Grants that have helped to pay for new programs for interoperability have come from a number of federal sources, notably from Department of Justice programs and, within the Department of Homeland Security (DHS), from the Federal Emergency Management Administration (Emergency Preparedness and Response Directorate) and the Office for Domestic Preparedness (ODP) in the Border and Transportation Security Directorate. Grant programs such as those at ODP for Urban Area Security and High-Threat Urban Areas are on-going.[37]

According to an undated fact sheet from DHS, since September 11, 2001, the Administration has allocated $200 million specifically for improving interoperability and $5.4 billion has been provided to states for emergency preparedness that could include interoperable communications.[38] The amount of dollars available, although significant, represents a small portion of the "several billions" that the Government Accountability Office (GAO) reports as the estimated sum needed to achieve interoperability.[39] The GAO concludes that "federal funding assistance programs to state and local governments do not fully support regional planning for communications interoperability."[40] One cause cited was the restraint on planning and budgeting imposed by limiting federal funding to annual grants only.

Provisions of the Intelligence Reform and Terrorism Prevention Act permit federal funding programs to make multi-year commitments for interoperable communications for up to three years, with a ceiling of $150 million for future obligations.[41] The act authorizes annual sums for a period of five years to be used for programs to improve interoperability and to assist interoperable capability in high-

---

[37] For full details, please refer to CRS Report RS21677, *Office for Domestic Preparedness Grants for 2004: State Allocation Fact Sheet*; CRS Report RL32696, *Fiscal Year 2005 Homeland Security Grant Program: State Allocations and Issues for Congressional Oversight;* and CRS Report RS22050, *FY2006 Appropriations for State and Local Homeland Security*, all by Shawn Reese. A report from the Government Accountability Office provides many details about funding for first responders, especially grants from ODP: *Management of First Responder Grant Programs and Efforts to Improve Accountability Continue to Evolve*, April 12, 2005, GAO-05-530T.

[38] Department of Homeland Security, "Fact Sheet:RapidCom 9/30 and Interoperability Progress" [http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0470.xml]. Viewed April 13, 2005.

[39] *Federal Leadership Needed to Facilitate Interoperable Communications Between First Responders*, Government Accountability Office, GAO-04-1057T, September 8, 2004, p. 16.

[40] Ibid, Highlights.

[41] P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (e).

risk urban areas; the 2005 authorization is $22,105,000; the amount rises each year to $24,879,000 in 2009.

Although the need for more funding appears to be at the top of almost any list regarding interoperable communications policy, many have expressed concern that there is no strategy that prioritizes what needs to be funded though federal programs, leading to waste and inequities. Two key bills deal with changing the formulas for appropriations for first responder and homeland security grants, with one objective the improvement of the effectiveness of grant dollars. The Senate bill (S. 21, Senator Collins) makes changes in the grants formula and also authorizes funds for first responders. The major House bill (H.R. 1544, Representative Cox) offers new formulas and guidelines but does not authorize specific dollar amounts.

Taking a different approach to funding, the Public Safety Interoperability Implementation Act (H.R. 1323, Representative Stupak) would establish in the U.S. Treasury a Public Safety Communications Trust Fund[42] to be funded in part with annual appropriations of $500 million for each of three fiscal years,[43] and in part with a percentage of certain spectrum auction proceeds.[44] The fund is to be administered by the NTIA, in consultation with a board of five directors appointed by the Secretary of Commerce. The board is to consult with the Department of Homeland Security, which may also be represented by one or more members on the board.[45] The NTIA Administrator is to make grants from the fund "to implement interoperability and modernization . . . for the communications needs" of public safety organizations and related agencies or entities.[46] Preference for grants is to be given to those proposing inter-agency or regional and multi-jurisdictional interoperability programs.[47]

High-Risk Urban Areas

The 9/11 Commission recommendation urged immediate funding of signal corps in high-risk urban areas to assure connectivity "among civilian authorities, local first responders, and the National Guard." The act responded by amending the Homeland Security Act to specify that DHS is to give priority to the rapid establishment of interoperable capacity in urban and other areas determined to be at high risk from terrorist attack. The Secretary of Homeland Security is required to work with the FCC, the Secretary of Defense, and appropriate state and local authorities to provide technical guidance, training, and other assistance as appropriate.[48] Minimum capabilities for "all levels of government agencies," first responders, and others include the ability to communicate with each other and to

---

[42] H.R. 1323, Sec. 3, 'Sec. 106 '(a) '(1).

[43] H.R. 1323, Sec. 3, 'Sec. 106 '(f).

[44] H.R. 1323, Sec. 3, 'Sec. 106 '(a) '(2).

[45] H.R. 1323, Sec. 3, 'Sec. 106 '(b) '(1).

[46] H.R. 1323, Sec. 3, 'Sec. 106 '(c) '(1).

[47] H.R. 1323, Sec. 3, 'Sec. 106 '(c) '(2).

[48] P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (d), 'Sec. 510 '(a).

have "appropriate and timely access" to the Information Sharing Environment, an initiative treated elsewhere in the act.[49]

The act further requires the Secretary of Homeland Security to establish at least two pilot programs in high threat areas. The process of development for these programs is to contribute to the creation and implementation of a national model strategic plan.[50] The purpose of this plan is to foster interagency communications at all levels of the response effort.[51] Building on the 9/11 Commission recommendation to use the resources of the Army Signal Corps, the Secretary is to consult with the Secretary of Defense in the development of the pilot projects, including review of standards, equipment, and protocols.[52] DHS was to have established at least two pilot projects in high threat or urban areas for interagency communications by March 2005;[53] as of the date of this report, this program is in review.

Underscoring the need to aid first responders in urban areas, H.R. 1795 (Representative Maloney) would require DHS to provide a communications system for the New York City Fire Department, including radios for the entire department and upgrades to its dispatch system. The bill specifies that such a network should be "seamless from the receipt of a 911 call to the dispatch of the firefighter,"[54] and interoperable with other public safety offices within the city.[55] Other systems requirements include being able to transmit a firefighter's identity and location;[56] sufficient capacity to send, in real time, data about buildings and property;[57] performance tested for operation in "all locations and under all conditions in which firefighters can reasonably be expected to work . . .".[58]

---

[49] P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (d), 'Sec. 510 '(b).

[50] P.L. 108-458, Title VII, Subtitle C, Sec. 7304 (a).

[51] P.L. 108-458, Title VII, Subtitle C, Sec. 7304 (b).

[52] P.L. 108-458, Title VII, Subtitle C, Sec. 7304 (d).

[53] P.L. 108-458, Title VII, Subtitle C, Sec. 7304 (a).

[54] H.R. 1795, Sec. 2 (11) (A).

[55] H.R. 1795, Sec. 2 (11) (B).

[56] H.R. 1795, Sec. 3 (b) (2) (B).

[57] H.R. 1795, Sec. 3 (b) (3) (C).

[58] H.R. 1795, Sec. 3 (c).

II. POLICY IMPLICATIONS

Policy and Planning

At a number of hearings throughout the 108th Congress,[59] and in reports by the Government Accountability Office,[60] the need for better governance and planning for interoperability was raised repeatedly. While not embracing the 9/11 Commission recommendation for a Signal Corps, the Intelligence Reform and Terrorism Prevention Act does include requirements for planning and for studies and reports that might lead to future changes in governance and national policy for interoperability and planning. The Administration also has asked for detailed studies and plans regarding spectrum use and communications for public safety.

Federal Planning

On November 30, 2004, President George W. Bush issued a memorandum to the heads of Executive Departments and agencies regarding steps to be taken to improve the management of spectrum assigned for federal use.[61] Most of these steps are to implement recommendations made by the Federal Government Spectrum Task Force in its report to the President in June 2004.[62] Among the deadlines provided in the memorandum are two requirements related specifically to public safety. One requirement is for the Secretary of Homeland Security to identify public safety spectrum needs by June 2005. The Secretary is to work with the Secretary of Commerce and, as needed, with the Chairman of the Federal Communications Commission; representatives from the public safety community; state, local, regional

---

[59] Hearing of the House of Representatives, Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet, "Protecting Homeland Security: A Status Report on Interoperability Between Public Safety Communications Systems," June 23, 2004; Hearing of the House of Representatives, Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations, "Public Safety Interoperability: Look Who's Talking Now," July 20, 2004; Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, "More Time, More Money, More Communication?" September 8, 2004; Hearing of Senate Committee on Commerce, Science and Transportation, "Spectrum for Public Safety Users," September 8, 2004.

[60] For example, *Challenges in Achieving Interoperable Communications for First Responders,* Government Accountability Office, GAO-04-231T, November 6, 2003; *Federal Leadership and Intergovernmental Cooperation Required to Achieve First Responder Interoperable Communications*, GAO-04-720, July 2004; *Federal Leadership and Intergovernmental Cooperation Required to Achieve First Responder Interoperable Communications*, GAO-04-963T, July 20, 2004; and *Federal Leadership Needed to Facilitate Interoperable Communications Between First Responders*, GAO-04-1057T, September 8, 2004.

[61] "Presidential Determination: Memorandum for the Heads of Executive Departments and Agencies," November 30, 2004, Office of the Press Secretary, News & Policies, at [http://www.whitehouse.gov/news/releases/2004/11/20041130-8.html]. Viewed April 26, 2005.

[62] *Spectrum Policy for the 21st Century: The President's Spectrum Policy Initiative*.

and tribal governments; and the private sector. Also, by year-end 2005, the Secretary of Homeland Security is to lead the preparation of a Spectrum Needs Plan, "to address issues related to communication spectrum used by the public safety community, as well as the continuity of Government operations." Concurrently, the Secretary of Commerce is to develop a Federal Strategic Spectrum Plan.

State Planning

The Intelligence Reform and Terrorism Prevention Act links grant-making with planning efforts in its provisions.[63] Requirements for planning for spectrum and interoperability in order to qualify for funding assistance include 1) description of available radio frequency uses and planned uses;[64] 2) description of how plans for spectrum use and interoperability are compatible with plans for "Federal, State and local governmental entities, military installations, foreign governments, critical infrastructure, and other relevant entities;"[65] and 3) inclusion of a five-year plan showing how resources will be used.[66] The language provides criteria for non-federal planners that could be expected to mesh with federal planning efforts required by the Administration and in other sections of the act.[67] Furthermore, additional provisions of the act require the Secretary of Homeland Security to establish at least two pilots to develop a "regional strategic plan to foster interagency communications," consistent with the national strategic plan to be developed at the request of Congress by the Secretary of Homeland Security.[68]

The strategic planning efforts required by Congress and by the Administration have similar goals. Although requirements for federal planning are more extensive than what has been asked of states and other non-federal entities, a possible synergy among the various programs could lead to the crafting of a nationwide plan with clearly defined links to state and local planning and to the private sector. A template for interoperability planning has been developed within DHS that could be used as a first step toward meeting the planning requirements set forth in the act.[69]

---

[63] Funding programs are covered in several CRS reports, including CRS Report RL32696, *Fiscal Year 2005 Homeland Security Grant Program: State Allocations and Issues for Congressional Oversight*, by Shawn Reese.

[64] P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (f) (2).

[65] P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (f) (3).

[66] P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (f) (4).

[67] Notably, P.L. 108-458, Title VII, Subtitle E, Sec. 7502.

[68] P.L. 108-458, Title VII, Subtitle C, Sec. 7304 (b).

[69] Statewide Communication Interoperability Planning (SCIP) Methodology, SAFECOM Program, Directorate of Science and Technology, Department of Homeland Security at [http://www.safecomprogram.gov/NR/rdonlyres/9628BE4B-E7A5-4F1B-9179-2CFCF2653CA9/0/SCIPMethodology.pdf]. Viewed April 13, 2005.

Policy and Technology

The act requires the Secretary of Homeland Security, the FCC, and the NTIA to conduct a study to assess strategies for public safety communications. The study is to include

- The need and efficacy of deploying nationwide interoperable communications networks.
- The capacity of public safety entities to use wireless broadband applications.
- The communications capabilities of all emergency response providers, including hospitals and health care workers, and current efforts to promote communications coordination and training among emergency response providers.[70]

Conclusions from this assessment might lead to recommendations for the development of a nationwide network for public safety, as many have advocated.[71] As has been noted by public safety communications experts, the federal government is but one operator of networks, in use or planned. There are also important networks operated or planned by states, and some private networks — such as those owned by utilities — that are accessible for public safety use. These networks could be linked through common interfaces to provide local, regional, or national coverage, as needed. The 9/11 Commission proposed a signal corps approach to public safety communications for high-risk urban areas. Such a capability would seem to include a system architecture to provide a backbone for wide area and local area networks and to support interoperability system-wide, as needed.

In addition to local gateways, communities — and the military — are testing leading edge technologies that can overcome problems of limited capacity of assigned frequencies, incompatible standards and other technical problems. The technologies being tested to improve interoperability include software-driven radios and smart antennae, mesh networks, and cognitive radio.

Software defined networks (radios, base stations, antennae) move wireless communications away from hard-wired equipment, where functionality is built into the components at the factory, by allowing changes in parameters to be downloaded remotely. Parameters that can be changed include standards and frequency assignments. Cognitive radio has the potential to eliminate entirely the need for frequency assignments. Cognitive radio is able to seek out and use any available frequency through miniaturized software programs contained within radio equipment.

---

[70] P.L. 108-458, Title VII, Subtitle E, Sec. 7502 (b).

[71] For example, testimony of Gary Grube, Chief Technology Officer, Motorola, Inc. at Hearing of Senate Committee on Commerce, Science and Transportation, "Spectrum for Public Safety Users," September 8, 2004.

Advanced versions of software-defined radio (SDR) being tested today are the building blocks for commercial applications of cognitive radio.

The Department of Defense, its agencies, and military departments have been leaders in research and development for software-programmable radios and base centers. These new technologies are expected to provide seamless interoperability in tactical operations and decrease the cost of infrastructure. A key program is the Joint Tactical Radio System (JTRS), designed to help the military migrate from its current wireless technology to SDR.[72] DOD is promoting the use of JTRS and its software communications architecture for homeland security and public safety communications and interoperability.[73]

Mesh networking is another promising technology that can facilitate public safety communications and interoperability. Mesh networks use radios that also act as mobile antennae, eliminating dependency on fixed antenna. Cities that are trying mesh networks for public safety include Medford, Oregon; San Mateo, California; North Miami Beach, Florida; and Garland, Texas.[74] The mesh network systems being installed for public safety in some communities and cities use proprietary standards and are not interoperable, echoing the proprietary, incompatible cellular radio networks that were developed in the last century to be the mainstay of today's mostly non-interoperable systems for public safety.

Other communities are using unlicenced spectrum to use Wi-Fi networks (fixed antennae) for public safety communications.[75] Using commercial, third-generation (3G) wireless technologies is also an option for first responders. New 3G phones offer high-speed Internet access and image transmissions as well as voice communications. Off-the-shelf camera phones can relay photos from an incident site to a command center, or vice versa. Advanced mobile phones are being prepared to receive multi-channel TV broadcasts in test markets. Interoperability for commercial wireless is supported by network backbones.

Convergence and Coordination

The concept of public safety communications is expanding as new technology makes it possible to include many whose role in preventing or responding to disaster lies outside the conventional definition of first responder. A more inclusive

---

[72] See [http://jtrs.army.mil/]. Viewed April 13, 2005.

[73] Overview at [http://jtrs.army.mil/sections/overview/fset_overview_domestic.html]. Viewed April 13, 2005.

[74] For more about mesh networks and public safety, see Government Computer News, "Oregon City Builds Mesh Network," May 24, 2004 and "Wireless Mesh Network Good as Gold," June 7, 2004, both by William Jackson.

[75] Wi-Fi, for wireless fidelity, operates on unlicensed frequencies. An example of how Wi-Fi can support public safety is the plan of Cook County, Illinois to implement Wi-Fi for public and private sector use. See "Metro Wi-Fi Finding Friends," by Ed Sutherland, Network Computing's Mobilepipeline, July 30, 2004 at [http://nwc.mobilepipeline.com/26100806]. Viewed April 13, 2005.

description of public safety responders might include utility workers (often among the first on the scene, to shut down power sources), health care workers other than those in emergency medical services, operators in 911 call centers, and bystanders at the scene of an accident or disaster. A Focus Group for the National Reliability and Interoperability Council (NRIC VII) suggests the term "emergency agency" and provides a suggested list of "agents" that might be part of an expanded "emergency response internetwork;" technology would provide the capability to link all parties and policy would determine the circumstances for, and type of, communication.[76]

A broader policy for public safety communications would include more types of communications capabilities as well as more participants and recipients. Although not included in its list of recommendations, the 9/11 Commission commented on the often inadequate response of the 911 call centers serving New York City,[77] and suggested "In planning for future disasters, it is important to integrate those taking 911 calls into the emergency response team and to involve them in providing up-to-date information and assistance to the public."[78] The absence of advance warning to communities inundated by the tsunami on December 26, 2004 provided a harsh reminder of the role of emergency alert systems — another form of public safety communications — in saving lives. The convergence of communications technology, typified by the near-ubiquity of the Internet and the wide availability of advanced wireless telephony, presages a world of end-to-end communications for public safety. These communications capabilities could incorporate a wide variety of systems and networks and be able to support almost any type of emergency response, emergency alert, or public safety information.

Another law passed in the 108th Congress, enacted in the same time frame as the Intelligence Reform and Terrorism Prevention Act, created an E-911 Implementation Coordination Office to foster improvements in 911 call centers.[79] Although no funding has been provided specifically for 911 programs, the existence of such an office at the federal level is a step toward coordinating 911 programs with emergency alert systems and other public safety programs. Separately, the Intelligence Reform and Terrorism Prevention Act contains two provisions for collecting information on emergency alert systems. One requires a study about the use of telecommunications networks as part of an all-hazards warning system, specifying that technologies to

---

[76] NRIC VII, Focus Group 1D, Communications Issues for Emergency Communications Beyond 911; Report #1 - Properties and network architectures that communications between PSAPs and emergency services personnel must meet in the near future ," December 6, 2004, pp. 12; 26-27. PSAPs are Public Safety Answering Points, also known as 911 Call Centers. NRIC is a Federal Advisory Committee chartered by the FCC, see Appendix. See [http://nric.org/meetings/docs/meeting_20041206/FG1D%20Final%20Report.pdf]. Viewed April 13, 2005.

[77] Final Report of the National Commission on Terrorist Attacks Upon the United States, Official Government Edition, 2004, pp. 286-287; 295; 306.

[78] *Op cit*., p. 318.

[79] P.L. 108-494, Title I.

consider would be "telephone, wireless communications, and other existing communications networks . . .".[80] The act also requires a pilot study using technology now being used for an Amber Alert network,[81] to improve public warning systems regarding threats to homeland security. This study and pilot, along with other pilots underway for public safety and emergency communications,[82] will add to the body of information and experience being created by the federal government and others.

Policy and Progress

The debate about public safety communications and the role of federal policy is long running. The framework for current discussions — which accommodate recent advances in technology — most likely dates to a report in 1996 by the Public Safety Wireless Advisory Committee (PSWAC).[83]

Some Recommendations from the Public Safety Sector

Listed below are some key components of a desirable public safety communications policy for first responders described in the PSWAC study and in more recent reports, testimony, and other comments cited in this report. According to these sources, a national policy for public safety communications needs to address and correlate a myriad of complex goals, such as

- Coordinated assignment and use of spectrum at various frequencies.
- Muscular and sustained efforts to complete the development and application of technical and operational standards.

---

[80] Requirement for Study Regarding Nationwide Emergency Notification System, Intelligence Reform and Terrorism Prevention Act, Title VII, Sec. 7403.

[81] An Amber Alert is used to locate missing children. It is named after Amber Hagerman, kidnaped and murdered in 1996; also referred to as the AMBER Plan, for America's Missing: Broadcast Emergency Response. websites with additional information include [http://www.amberalertnow.org], [http://www.amberalert911.org] and the site of the National Center for Missing and Exploited Children [http://www.ncmec.org]. All sites viewed April 26, 2005. See also CRS Report RS21453, *Amber Alert Program Technology*, by Linda K. Moore. The program and policy issues are discussed in CRS Report RL31655, *Missing and Exploited Children: Overview and Policy Concerns*, by Edith Cooper.

[82] Some key programs are discussed in the Appendix. See also CRS Report RL32527, *Emergency Communications: The Emergency Alert System (EAS) and All-Hazards Warnings*.

[83] The Public Safety Wireless Advisory Committee (PSWAC) was chartered in 1995, at the request of Congress, to study public safety spectrum and make recommendations for meeting spectrum needs through the year 2010. The following year, PSWAC submitted a report containing recommendations for the improvement of public safety communications over wireless networks. *Final Report of the Public Safety Wireless Advisory Committee*, September 11, 1996.

- Public sector adaptation of new technologies already available in the private sector such as for high-speed, data rich, and video or image transmissions.

- Long-term support of research and development for new technology.

- Coherent goals that encourage private investment in technology development.

- Nationwide network of communications operations centers (regional signal corps) that can serve as back-up facilities to each other and to state and interstate centers and networks.

- Interoperability of communications among first responders and public safety agencies.

- Managerial structure that can successfully coordinate not only disparate federal, state, and local agencies but also the different cultural and technical needs of independent first responder units.

- Framework to match policy goals with implementation needs to assure the effectiveness of federal funding for programs and grants.

Provisions in the Intelligence Reform and Terrorism Prevention Act

Congress has responded with provisions in the Intelligence Reform and Terrorism Prevention Act that provide specific instructions to federal departments and agencies to take actions to meet many of the goals outlined above, as well as respond to other concerns articulated by the public safety community. Key tasks that the act requires for public safety communications include

- Sense of Congress that it must pass legislation that resolves spectrum release as part of the transition to digital television; first session. Sec. 7501.

- Requirement for a study on spectrum for public safety and homeland security; December 2005. Sec. 7502 (a).

- Requirement for a study on strategies to meet interoperable communications needs; December 2005. Sec. 7502 (b).

- Report on plan to accelerate development of national interoperable standards, including milestones and achievements; April 2005. Sec. 7303 (b).[84]

---

[84] Responding to a CRS inquiry on status, DHS has indicated that the report has been completed and is in review.

- Establishment by the President of a mechanism for coordinating cross-border interoperability issues with Canada and Mexico; June 2006. Sec. 7303 (c).

- Requirement to establish at least two pilot projects in high threat or urban areas for interagency communications; March 2005. Sec. 7304 (a).[85]

- Reports on interagency communications pilots; interim, June 2005; final June 2006. Sec. 7304 (e).

- Authorization of funds for interoperable communications projects within DHS (not grant funds); fiscal years 2005 through 2009. Sec. 7303 (a) (3).

- Requirement for a study on the use of telephone, wireless and other existing communications networks as a means of providing a nationwide emergency notification system; September 2005. Sec. 7403.

- Requirement for a pilot study using a warning system similar to the Amber Alert communications network (using funds made available for improving the national warning system regarding terrorist attacks) with a report on findings and recommendations; September 2005. Sec.7404.

Some Key Requirements in Presidential Memorandum on Spectrum Use

Partly concurrent with requirements from Congress regarding improved communications and spectrum use are a number of federal programs and deadlines set by the President.[86] Requirements with near-term deadlines that have a bearing on public safety are

- Requirement for the Office of Management and Budget (OMB) to provide guidance for federal agencies regarding the identification of spectrum requirements and the costs of investments in spectrum-related programs; May 2005.

- Requirement for agencies to implement methods recommended by OMB, including steps to ensure greater consideration of more efficient and cost-effective spectrum use; November 2005.

---

[85] Responding to a CRS inquiry on status, DHS has indicated that the pilot project program is being reviewed.

[86] "Presidential Determination: Memorandum for the Heads of Executive Departments and Agencies," November 30, 2004, Office of the Press Secretary, News & Policies, at [http://www.whitehouse.gov/news/releases/2004/11/20041130-8.html]. Viewed April 26, 2005.

- Requirement for the Secretary of Commerce to provide agency-specific strategic spectrum plans; November 2005.

- Requirement for the Secretary of Homeland Security to identify public safety spectrum needs; May 2005.

- Requirement for the Secretary of Homeland Security to develop a comprehensive plan — the Spectrum Needs Plan — to address issues that include spectrum use by the public safety community; November 2005.

What's Been Accomplished

A survey of recent, key federal actions in areas concerning interoperability might be summarized as follows

- Participation in a number of demonstration projects (for example, Homeland Security Urban Area Security Initiative).

- Planning for rationalization and improvement of federal communications networks (for example, Integrated Wireless Network).

- Conducting pilot, part of the Integrated Public Alert and Warning System (IPAWS), to test an all-digital emergency alert network. This project may be expanded to include the Congressional requirement for a pilot using Amber Alert technology.

- [87]Provision of planning tools and consultative services to state and local first responders (for example, SAFECOM programs).

- Assistance in improving standards (for example, requirements for compatibility with Project 25 standards) and identifying needs for standards (for example, SAFECOM's requirements documents).

- Improvements in spectrum management for public safety (for example, FCC creation of the National Coordinating Committee and plans for rebanding to reduce interference on public safety radio channels).

- Increased funding to grants programs for first responders (for example, funding from the Office of Domestic Preparedness).

---

[87] Testimony of Michael D. Brown, Under Secretary of Homeland Security for Emergency Preparedness and Response, "Federal Emergency Management Agency," House of Representatives, Committee on Appropriations, Subcommittee on Homeland Security, March 9, 2005.

- Planned studies and pilots required by Congress and the Administration (noted above).
-

Issues for the 109th Congress

By its requirements for studies on interoperability strategies, use of technology, spectrum use, and more, Congress has assigned itself a number of specific tasks of oversight. Congress also has recognized the many dilemmas faced by its constituents in supporting communications interoperability. It has in many ways taken on the role of champion in support of programs for interoperability that benefit local communities, states and tribes. Many steps have been taken, particularly within DHS, and Congress has demanded further advances. Despite indications of progress, much remains to be done. Issues that could be addressed — collectively or singly — by Congress, the Administration, the private sector, or others include the development of a long term strategy that coordinates both public safety spectrum needs and interoperable communications needs, and the coordination of the various studies requested by Congress and by the Administration. The findings and recommendations from these studies are crucial to the advancement of policy for public safety.

The achievement of a comprehensive set of solutions for interoperability outside the federal government appears to remain elusive. Participation of the federal government in a national solution for interoperability does not necessarily require federal ownership. The federal government is an important component, however, of any network that might be put in place to provide interoperable communications. In light of the critical role of federal participation, Congress could decide to extend its oversight role to include incremental progress reports on programs such as those noted above, in advance of the deadlines it has set for required studies.

Appendix I - Federal Administration

The key federal agencies for spectrum management and first responder communications are the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA). Among other responsibilities, the FCC supervises spectrum for non-federal public safety agency communications. The NTIA — part of the Department of Commerce — administers spectrum used by federal entities. The lead federal program for fostering interoperability is administered by the Wireless Public SAFEty Interoperable COMmunications Program, dubbed Project SAFECOM,[88] part of the Department of Homeland Security.[89] SAFECOM has not to date played a major role in spectrum policy. DHS has created an Office of Interoperability and Compatibility (OIC) of which SAFECOM is a part. In June 2004 DHS announced the creation of a Regional Technology Integration Initiative. DHS has also announced the organization of a National Incident Management System (NIMS) in response to a Presidential Directive (HSPD-5).[90] A NIMS Integration Center is planned to deal with compatibility and will be responsible for at least some interoperable communications.

National Telecommunications and Information Administration

To address the need for interoperability spectrum, in June 1999 the NTIA designated certain federally-allocated radio frequencies for use by federal, state, and local law enforcement and incident response entities. The frequencies are from exclusive federal spectrum, and are adjacent to spectrum used by state and local governments. NTIA's "interoperability plan," — developed in coordination with the Interdepartmental Radio Advisory Committee (IRAC)[91] — is used to improve communications in response to emergencies and threats to public safety. In 1996, the NTIA created a public safety program to coordinate federal government activities for spectrum and telecommunications related to public safety. Today, its successor, the Public Safety Division of the Office of Spectrum Management, participates in various initiatives to improve and coordinate public safety communications. The Division is preparing a *Spectrum Efficiency Study* and an *Interoperable Communications Summary Guide*.[92] Two forums on public safety and spectrum use have been sponsored by the NTIA, one in June 2002 and another in February 2004.[93]

---

[88] Additional information is at [http://www.safecomprogram.gov/].

[89] DHS is the managing partner for the SAFECOM program. Contributing partners include these Departments: Justice, Treasury, Transportation, Defense, Agriculture, Energy, Health and Human Services, and Interior.

[90] Full document at [http://www.dhs.gov/interweb/assetlibrary/NIMS-90-web.pdf]. Viewed April 13, 2005.

[91] IRAC, with representation from 20 major federal agencies, develops policies for federal spectrum use, and represents the United States at International Telecommunications Union conferences. See [http://www.ntia.doc.gov/osmhome/irac.html]. Viewed April 13, 2005.

[92] Additional information at [http://ntiacsd.ntia.doc.gov/pubsafe/]. Viewed April 13, 2005.

[93] Agenda and reports of the 2004 Public Safety Forum are available at (continued...)

Federal Communications Commission

Over roughly the last 20 years, the FCC has initiated several programs that involve state, local, tribal and — usually — private sector representatives. In 1986, it formed the National Public Safety Planning Advisory Committee to advise it on management of spectrum in the 800 MHZ band, newly designated for public safety. The following year, the FCC adopted a Public Safety National Plan that, among other things, established Regional Planning Committees (RPCs) to develop plans that met specific needs. The FCC encourages the formation of RPCs with a broad base of participation. The RPCs have flexibility in determining how best to meet state and local needs, including spectrum use and technology.

The regional planning approach is also being applied to spectrum in the Upper 700 MHz band.[94] Technical and operational standards, including interoperability standards, were developed and recommended to the FCC through the Public Safety National Coordination Committee (NCC). Standards for narrowband radio applications, for example, were recommended to the FCC and adopted in early 2001. Established by the FCC in 1999 and ended in 2003, the NCC had a Steering Committee from government, the public safety community, and the telecommunications industry.

Homeland Security. Among actions by the FCC specifically in support of homeland security were the chartering of the Media Security and Reliability Council (MSRC)[95] and the renewal of the charter for the Network Reliability and Interoperability Council (NRIC).[96] Both of these are Federal Advisory Committees. MSRC has been active in evaluating the effectiveness of the Emergency Alert System. The primary role of NRIC is to develop recommendations for best practices for private sector telecommunications to insure optimal reliability, interoperability, and connectivity of networks. The current NRIC focus groups are: Near Term Issues, E911; Long Term Issues, E911; Best Practices, E911 and Public Safety; Emergency Communications Beyond E911; Best Practices, Homeland Security - Infrastructure; Best Practices, Homeland Security - CyberSecurity; Best Practices, Wireless Industry; Best Practices, Public Data Networks; and Broadband.

Spectrum and Interoperability. The FCC's strategic goal for spectrum is to "Encourage the highest and best use of spectrum domestically and internationally in order to encourage the growth and rapid deployment of innovative and efficient communications technologies and services."[97]

---

[93] (...continued)
[http://www.ntia.doc.gov/ntiahome/ntiageneral/specinit/forum2/]. Viewed April 13, 2005.

[94] See [http://wireless.fcc.gov/publicsafety/700MHz]. Viewed April 13, 2005.

[95] See [http://www.fcc.gov/MSRC/Welcome.html]. Viewed April 13, 2005.

[96] See [http://www.nric.org].

[97] See [http://www.fcc.gov/omd/strategicplan/#goals]. Viewed April 13, 2005.

Regarding interoperability, the FCC describes its role as "directing efforts toward allocating additional spectrum for public safety systems, nurturing technological developments that enhance interoperability and providing its expertise and input for interagency efforts such as SAFECOM."[98] However, the FCC asserts that there are limitations on what it can do. "The Commission is only one stakeholder in the process and many of the challenges facing interoperability are a result of the disparate governmental interests . . . making it difficult to develop and deploy interoperable strategies uniformly."[99]

Department of Homeland Security, Office of Interoperability and Compatibility

The function of the Office of Interoperability and Compatibility (OIC) is to address the larger issues of interoperability. Among the goals of the OIC is the "leveraging" of "the vast range of interoperability programs and related efforts spread across the Federal Government" to "reduce unnecessary duplication" and "ensure consistency" in "research and development, testing and evaluation (RDT&E), standards, technical assistance, training, and grant funding related to interoperability." To achieve this, DHS will create within OIC "a series of portfolios to address critical issues." The OIC's initial priorities are for communications (SAFECOM), equipment, training and "others as required." To fulfill the portfolios, OIC will use a "systems engineering or lifestyle approach" to create "action plans." These will be "developed through a collaborative process that brings together the relevant stakeholders to provide clear direction on a path forward." This "end-user" input is expected to produce "a strategy and action plan" for each portfolio.[100] No time line for accomplishing these planned steps has of yet been provided,

SAFECOM. With the support of the Administration, Project SAFECOM was designated the umbrella organization for federal support of interoperable communications. It was agreed within DHS that SAFECOM would be part of the Science and Technology Directorate, in line with a policy for placing technology prototype projects under a single directorate; this decision was reportedly based on the research-oriented nature of the programs envisioned for SAFECOM by its administrators.[101] The Intelligence Reform and Terrorism Prevention Act affirmed this decision by giving DHS the authority to create an office for interoperability

---

[98] Testimony of John B. Muleta, Chief, Wireless Telecommunications Bureau, Federal Communications Commission at Hearing of the House of Representatives, Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, "More Time, More Money, More Communication?" September 8, 2004.

[99] Ibid.

[100] Testimony of Dr. David G. Boyd, Program Manager, SAFECOM, Department of Homeland Security, Hearing of the House of Representatives, Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations, "Public Safety Interoperability: Look Who's Talking Now," July 20, 2004.

[101] "Homeland Security Starting Over With SAFECOM," Government Computer News, June 9, 2003.

within the Science and Technology Directorate and to manage SAFECOM as part of that effort.[102] SAFECOM recently released a template for interoperability planning that can be used by states to establish a strategy for interoperability[103] and is preparing a methodology to establish a baseline for interoperability achievements as an evaluation tool to measure the success of future interoperability programs. Reportedly, SAFECOM will release initial findings on the baseline measurement some time in 2005.[104]

SAFECOM absorbed the Public Safety Wireless Network (PSWN) Program, previously operated jointly by the Departments of Justice and the Treasury. PSWN was created to respond to recommendations made by the Public Safety Wireless Advisory Committee regarding the improvement of public safety communications over wireless networks. PSWN operated as an advocate for spectrum management policies that would improve wireless network capacity and capability for public safety. SAFECOM, however, has no authority over spectrum management decisions. The following quote is a summary of SAFECOM's position on spectrum policy.

> Spectrum policy is an essential issue in the public safety communication arena. Unfortunately, State and local public safety representatives are frequently not included in spectrum policy decisions, despite their majority ownership of the communications infrastructure and their importance as providers of public and homeland security. SAFECOM will hence play a role in representing the views of State and local stakeholders on spectrum issues within the Federal Government. Last year, SAFECOM was appointed to an interagency Spectrum Task Force to contribute such views, and the ongoing working relationship that has developed between SAFECOM and the FCC will, we believe, pay huge dividends in the future.[105]

Regional Technology Integration Initiative

In June 2004, the Directorate of Science and Technology introduced a new initiative to facilitate the transition of innovative technologies and organizational concepts to regional, state, and local authorities.[106] The initiative has selected four urban areas from among those currently part of the Homeland Security Urban Area Security Initiative. Two of the areas that have been reported as choices are

---

[102] P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (a) (2).

[103] Statewide Communication Interoperability Planning (SCIP) Methodology, SAFECOM Program, Directorate of Science and Technology, Department of Homeland Security at [http://www.safecomprogram.gov/files/SCIP_Methodology_FINAL.pdf]. Viewed April 26, 2005.

[104] "Safecom SCIPs Across States," by Dibya Sarkar, FCW.com, January 7, 2005.

[105] Boyd, Hearing, July 20, 2004.

[106] DHS Press Releases, including "Homeland Security Launches Regional Technology Integration Initiative in Seattle," February 18, 2005 [http://www.dhs.gov/dhspublic/display?content=4362] and "Fact Sheet: Regional Technology Initiative" at [http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0430.xml]. Viewed April 26, 2005.

Cincinnati, Ohio and Anaheim, California.[107] Each area will reportedly receive $10 million to expand new systems that test more advanced technologies for public safety communications, including interoperability. Anaheim, for example, reportedly has created a virtual operations center (instead of a building), relying on network technology to connect police, fire, medical services and public utilities in case of an emergency. The announced goal is to get all who respond to disasters and other emergencies to work from a common base.[108]

National Incident Management System

NIMS also has announced plans to address questions of interoperability and communications, although no mention of spectrum policy is mentioned in the DHS report on NIMS issued March 1, 2004.[109] The objective for communications facilitation is summarized as "development and use of a common communications plan and interoperable communications processes and architectures."[110] NIMS envisions mandatory compliance with "national interoperable communications standards, once such standards are developed."[111] These standards will include interoperable wireless communications for "Federal, State, local and tribal public safety organizations."[112]

Integrated Wireless Network

The Integrated Wireless Network (IWN) for law enforcement is being planned as a joint program by the Departments of Justice, the Treasury, and Homeland Security. DHS is represented in the IWN Joint Program Office through the Wireless Management Office of the Chief Information Officer.[113] IWN, from its description, will have limited interoperability at the state and local level. The described objective of IWN is network integration for "the nation's law enforcement wireless communication, and data exchange capability through the use of a secure integrated wireless network."[114]

---

[107] "Department of Homeland Security funding initiative aims to spur interoperability among locals," by Jim McKay, Government Technology, September 2004, p. 1.

[108] Ibid.

[109] "National Incident Management System," Department of Homeland Security, March 1, 2004, at [http://www.dhs.gov/interweb/assetlibrary/NIMS-90-web.pdf]. Viewed April 13, 2005.

[110] Ibid, p. 11.

[111] Ibid, p. 50.

[112] Ibid., p. 52.

[113] Memorandum of Understanding Between the Department of Homeland Security, the Department of Justice, and the Department of the Treasury Regarding a Joint Tactical Wireless Communications System, at [http://www.usdoj.gov/jmd/iwn/schedule.html]. Viewed April 14, 2005.

[114] Request for Comment, Draft Phase 2 Request for Proposals, October 13, 2004, C.2.3 (a), page 8 at [http://www.usdoj.gov/jmd/iwn/schedule.html]. Viewed April 14, 2005.

Other Coordinating Bodies

SAFECOM has created a Federal Interoperability Coordination Council (FICC), made up of "all the federal agencies with programs that address interoperability."[115] Previously, as part of its e-government mandate to rationalize federal programs for interoperability, SAFECOM met with representatives from 60 different programs operated by the federal government or funded by or partnered with a federal agency. Many of these programs include state committees and national associations such as the Association of Public-Safety Communications Officials - International (APCO).[116] Part of the National Coordination Committee's mission was to encourage the creation of Statewide Interoperability Executive Committees (SIEC),[117] to take part in coordination efforts. The National Public Safety Telecommunications Council (NPSTC) is another important coordinating body. NPSTC unites public safety associations to work with federal agencies, the NCC, SIECs and other groups to address public safety communications issues.[118] It has been supported by the AGILE Program, created by the National Institute of Justice (NIJ).[119] AGILE has addressed interim and long-term interoperability solutions in part by testing standards for wireless telecommunications and information technology applications. The AGILE Program also has provided funding to Regional Planning Committees for start-up costs and the preparation and distribution of regional plans. AGILE is being restructured, to be replaced by a more limited function in Communications Technology, CommTech. CommTech is not designed to play a primary role in coordinating interoperability policy within the public safety community.

The SIECs, NPSTC, Regional Planning Committees and other federally-supported but not federally-directed organizations play key roles as facilitators in advancing programs for public safety communications. In recent testimony quoted above,[120] both SAFECOM and the FCC have described their roles primarily as facilitators also. SAFECOM and DHS, in its plans for the Office of Interoperability and Compatibility, seem to place a high priority on consultative functions. It appears that OIC policy will focus on portfolios of recommendations for achieving interoperability at an incident site and not on establishing the higher levels of interoperability provided by network support and back-up from regional

---

[115] Testimony of Dr. David G. Boyd, Program Manager, SAFECOM, Department of Homeland Security, Hearing of the House of Representatives, Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, "More Time, More Money, More Communication?" September 8, 2004.

[116] See [http://www.apcointl.org/].

[117] A discussion of the role of SIECs, and a recommendation to mandate their use, is contained in testimony by Stephen T. Devine, Missouri SIEC Chairperson, Missouri State Highway Patrol, at Hearing of the House of Representatives, Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations, "Public Safety Interoperability: Look Who's Talking Now," July 20, 2004.

[118] Information at [http://npstc.du.edu/].

[119] AGILE stands for Advanced Generation of Interoperability for Law Enforcement. See [http://www.agileprogram.org/justnet.html]. Viewed April 13, 2005.

[120] Boyd and Muleta, Hearing, July 20, 2004.

communications command centers. In its discussions of Emergency Operations Centers and Incident Command Systems, however, NIMS seems to indicate the need for a national network architecture and fixed as well as mobile operations centers for communications network support. The Regional Technology Integration Initiative has been established to act as a catalyst between existing technology used by first responders and the innovative technology needed in the future. It seeks to work at the local, state and regional levels but appears to favor solutions that can be applied on a regional basis.